(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 48 501 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
G 06 F 3/037
G 07 C 9/00

(21) Aktenzeichen: 198 48 501.8
(22) Anmeldetag: 21. 10. 1998
(43) Offenlegungstag: 4. 5. 2000

(71) Anmelder:
sfr Gesellschaft für Datenverarbeitung mbH, 50825 Köln, DE

(74) Vertreter:
Wagner, M., Dipl.-Ing., Pat.-Anw., 52068 Aachen

(72) Erfinder:
Schöttler, Winfried, 50733 Köln, DE

(56) Entgegenhaltungen:
DE 196 20 346 A1
US 55 59 961

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Identitätsprüfung

(57) Es ist ein Verfahren zur Identitätsprüfung mittels Paßwort offenbart, bei dem das Paßwort durch Auswahl bestimmter Details/Regionen eines Bildes generiert wird. Dieses Verfahren hat neben der leichteren Erinnerbarkeit der Paßwörter insbesondere den Vorteil, daß es auch in Systemen ohne Tastatur z. B. "Touchscreen" eingesetzt werden kann.

DE 198 48 501 A 1

Beschreibung

Die meisten Betriebssysteme und viele Programme verlangen, daß der Benutzer sich identifiziert. In der Regel geschieht dies durch Eingabe eines Paßworts (Eingabe von Text). Aus Sicherheitsgründen sollen diese Paßwörter möglichst nicht assoziativ gebildet werden (NICHT der Vorname der Kinder, NICHT der Hochzeitstag, etc.). Aus dem gleichen Grund ist eine Änderung der Paßwörter in regelmäßigen Abständen erwünscht.

Die meisten Computerbenutzer müssen daher mit einer größeren Zahl schlecht memorierbarer, ständig wechselnder Paßwörter leben. Die Folge sind gravierende Sicherheitslükken, da einzelne Anwender entweder die oben skizzierten Regeln außer acht lassen oder sich ihre Paßwörter mehr oder weniger öffentlich zugänglich notieren.

Ein weiterer Nachteil text- oder ziffernbasierter Paßwörter ist die Möglichkeit, daß Dritte durch aufmerksames Beobachten der Eingabe das Paßwort "lesen" können.

Zur einfachen und kostengünstigen Beseitigung der skizzierten Nachteile ist eine Anordnung bekannt geworden (vgl. EP 0 677 801 A1), bei der Bilder zur Eingabe eines Paßwortes verwendet werden. Menschen fällt es wesentlich leichter, sich an Bilder (Bildteile) als an Text zu erinnern. Zudem sind die Assoziationen zu Bildern wesentlich vielfältiger und individueller als dies bei Texten der Fall ist. Die Eingabe des Paßworts erfolgt dort dadurch, daß innerhalb der Bilddarstellung bei der Ersteingabe eine Region ausgewählt und bei den Folgeeingaben überprüft wird, ob die Neueingabe innerhalb einer bestimmten Toleranz liegt.

Nachteilig bei diesem Verfahren ist es, daß die Regionen regelmäßig z. B. quadratisch und somit von festgelegter Form sind und im schlechtesten Fall auch noch nach Art eines Rasters angeordnet sind. Die Erinnerbarkeit derartiger Regionen ist schlecht, da sie in keinem Zusammenhang mit dem Bild, auf dem sie sich befinden, stehen.

Außerdem ist nachteilig, daß durch die Abspeicherung von Geometriedaten (Koordinaten, Vektoren) keine Anbindung an herkömmliche z. B. Kryptographieverfahren möglich ist.

Aufgabe der vorliegenden Erfindung ist es daher, unter Vermeidung der aus dem Stand der Technik bekannten Nachteile ein Verfahren zu schaffen, mit dem einfach und kostengünstig eine wirksame und sichere Identitätsprüfung ermöglicht wird.

Diese Aufgabe wird mit einem Verfahren nach dem Hauptanspruch gelöst, das die folgenden Schritte umfaßt:

- erstes Anzeigen eines sichtbar oder unsichtbar in verschiedene Regionen gegliederten Bildes;
- Zuordnen eines alphanumerischen od. dgl. Zeichens zu der von einem Benutzer bei einer Ersteingabe ausgewählten, mindestens einen Region;
- Abspeichern des Zeichens;
- Anzeigen des unsichtbar in verschiedene Regionen gegliederten Bildes;
- Zuordnen eines alphanumerischen od. dgl. Zeichens der von dem Benutzer bei einer folgenden Eingabe ausgewählten, mindestens einen Region;
- Vergleichen des Zeichens der ausgewählten Region mit dem abgespeicherten Zeichen; und
- Feststellen der Identität des Benutzers, falls das Zeichen der ausgewählten Region mit dem abgespeicherten Zeichen übereinstimmt.

Die Eingabe des Paßworts erfolgt also durch die Auswahl (z. B. durch Anklicken mit dem Mauszeiger) einzelner Symbole oder Regionen eines Bildes. Diese Vorgehensweise hat neben der bereits skizzierten leichteren Erinnerbarkeit der Paßwörter weitere Vorteile:

- Das Verfahren kann auch in Systemen ohne Tastatur ("Touchscreen", Kiosksysteme) eingesetzt werden.
- Im Vergleich zu anderen Identifizierungssystemen, wie z. B. biometrischen Verfahren, ist in der Regel keine zusätzliche Hardware erforderlich, da heute praktisch alle Rechnersysteme mit einer Maus, einem Joystick, einem Trackball oder einem vergleichbaren Eingabegerät ausgestattet sind.
- Im Gegensatz zu biometrischen Verfahren besteht kein direkter Zusammenhang zwischen den Merkmalen der Identifizierung und der sich identifizierenden Person, d. h. dasselbe Paßwort kann sogar von mehreren Personen benutzt werden.

Vorteilhafte Ausgestaltungen des Verfahrens sind Gegenstand der Unteransprüche.

So ist es bevorzugt, wenn mehrere Regionen bei der Ersteingabe ausgewählt, die entsprechenden Zeichen gespeichert und bei einer folgenden Eingabe mit den Zeichen der dann ausgewählten Regionen verglichen werden. Hierdurch verringert sich die Wahrscheinlichkeit für "Zufallstreffer" bei Manipulationsversuchen.

Diese kann weiter dadurch positiv beeinflußt werden, daß bei der Ersteingabe auch die Reihenfolge der Zeichen der ausgewählten Regionen abgespeichert wird und der Zugang nur dann gewährt wird, wenn auch die Reihenfolge der Zeichen der von dem Benutzer bei einer folgenden Eingabe ausgewählten Regionen mit der abgespeicherten Reihenfolge der Zeichen übereinstimmt. Hierdurch erhält man also ein aus mehreren Zeichen bestehendes "Paßwort" im herkömmlichen Sinne.

Besonders vorteilhaft ist es, wenn die Zeichen der Regionen bei der Ersteingabe und den weiteren Verfahrensschritten nach Wahl des Benutzers aus verschiedenen Alphabeten entstammen. Dies können insbesondere zwei Alphabete, und hier wiederum insbesondere ein Großbuchstaben- und ein Kleinbuchstabenalphabet sein.

Weiter ist es vorteilhaft, wenn mehrere Bilder zur Auswahl stehen. Hierdurch wird wiederum die Gefahr von Zufallstreffern verringert.

Besonders vorteilhaft kann es sein, wenn ein Bild nach Auswahl durch einen ersten Benutzer für weitere Benutzer nicht mehr zur Auswahl steht. Für den ersten Benutzer muß dann eine erste z. B. herkömmliche Identitätsprüfung stattfinden, um ihm sein "persönliches" Bild zur Eingabe des Paßwortes anzuzeigen.

In der Folge wird beispielhaft anhand eines Verfahrens zur Überprüfung der Zugangsberechtigung zu einem PC eine bevorzugte Ausführungsform erläutert:
Eine Anlage zur Überprüfung der Identität bzw. Zugangsberechtigung weist z. B. einen üblichen PC, einen Bildschirm zur Anzeige der Bilder und ein Eingabegerät wie z. B. eine Maus auf.

Bei der Definition eines Paßwortes (Ersteingabe) wählt der Benutzer zunächst aus vorzugsweise zahlreichen angezeigten Bildern eines aus. Der Inhalt des Bildes ist beliebig, sollte nach Möglichkeit aber eine Vielzahl von Details wie markante Punkte, Symbole, farbige Flächen od. dgl. aufweisen. Das gleiche Bild erhält er später angezeigt, wenn er sich identifizieren soll.

Anschließend wählt der Benutzer mit der Maus oder einem anderem Eingabegerät einzelne Details des Bildes aus. Das Paßwort wird nun aus den gewählten Details und der Reihenfolge ihrer Auswahl gebildet.

Die gewählten Details und ihre Reihenfolge können leicht

erinnert werden. Zusätzlich hilft das Bild dem Gedächtnis, individuelle Assoziationsketten zu bilden. Darüber hinaus können auch einfache Merksätze die Erinnerung unterstützen: "Hund, Katze, Maus", "Das BOOT fährt auf dem FLUSS an dem MANN vorbei, der vor dem HAUS steht".

Zur Identifizierung wählt der Benutzer später aus dem vorgegebenen Bild die gleichen Symbole in der gleichen Reihenfolge.

Die eigentliche Umsetzung der Bildauswahl zu einem Paßwort erfolgt intern und vom Benutzer unbemerkt. Bei der Definition eines Paßwortes wird das gewählte Bild zunächst (für den Benutzer nicht zwingend sichtbar) in einzelne Flächen unterteilt. Die Gesamtzahl der Flächen steht für den maximalen Zeichenvorrat (das "Alphabet") des Paßworts; jede Fläche entspricht einem einzelnen Zeichen aus diesem Vorrat.

Die vom Benutzer zur Definition seines Paßwortes ausgewählten beliebigen Punkte des Bildes werden anschließend dem entsprechenden Zeichen zugeordnet und anschließend in das Paßwort übernommen. Die oben erwähnte Auswahl der vier Details [BOOT] [FLUSS] [MANN] [HAUS] könnte so z. B. zu dem Vierzeichen-Paßwort "HZPÜ" führen.

Dem Benutzer kann dabei die Möglichkeit eingeräumt werden, z. B. durch Anklicken der Bildregionen mit der rechten oder linken Maustaste, Einfluß auf die Zeichen des Paßworts zu nehmen, z. B. die Groß- und Kleinschreibung beeinflussen. So könnte z. B. die Auswahl der Details [BOOT/rechte Maustaste] [FLUSS/rechte Maustaste] [MANN/rechte Maustaste] [HAUS/rechte Maustaste] wie oben zu dem Paßwort "HZPÜ", die Auswahl der Details [BOOT/rechte Maustaste] [FLUSS/linke Maustaste] [MANN/rechte Maustaste] [HAUS/linke Maustaste] jedoch zu dem Paßwort "HzPü" führen.

In jedem Falle identifiziert sich der Benutzer später dadurch, daß er die gleichen Punkte/Details/Regionen in der gleichen Reihenfolge und mit den gleichen zusätzlichen Aktionen (recht/linke Maustaste) auswählt, wodurch intern das gleiche Paßwort gebildet wird.

Für die Aufteilung der Graphik in Flächen sind zwei Verfahren möglich:

Regelmäßige Aufteilung

Die Gesamtfläche wird in regelmäßige Zellen aufgeteilt (z. B. in Rechtecke oder Sechsecke). Bei der Definition des Paßworts wird dieses Gitter für jede separate Eingabe so verschoben, daß der gewählte Punkt der Grafik genau in der Mitte einer Zelle liegt. Hierdurch wird die notwendige "Unschärfe" einer späteren Eingabe kompensiert. Niemand kann immer exakt den gleichen Punkt einer Grafik anwählen. Die Größe der Gitterzellen entspricht daher dem Bereich, innerhalb dessen eine Eingabe gültig bleibt. Eine Verschiebung des gesamten Gitters ist notwendig, um Abweichungen in jeder Richtung zu erlauben.

Neben der Graphik müssen die Größe der Zellen und die Offsets der einzelnen Gitterverschiebungen gespeichert werden, um später aus der Benutzereingabe das korrekte Paßwort bilden zu können. Die Sicherheit des Paßwortes ist von der Größe der einzelnen Zellen abhängig, da durch sie implizit die Gesamtzahl der Zellen festgelegt wird (Umfang des Alphabets).

Die regelmäßige Aufteilung der Graphik ist in der **Fig. 1** schematisch dargestellt.

Unregelmäßige Aufteilung

Die unregelmäßige Aufteilung einer Graphik kann auf die Besonderheiten des dargestellten Inhalts eingehen (markante Punkte, einzelne Symbole, auffällige Flächen). Die Aufteilung der Maske erfolgt in diesem Fall entweder manuell oder durch entsprechend "intelligente" Programme. Im Gegensatz zum ersten Verfahren entfällt das Merkmal einer nicht spezifischen "Unschärfe". Zwischen dem Benutzer und dem Hersteller der Maske müssen daher Vereinbarungen getroffen werden, wie einzelne Symbole ausgewertet werden (z. B. "Kante oder Fläche").

Neben der Grafik muß die komplette Maske (das Alphabet) gespeichert werden. Auch hier ist die Sicherheit des Paßwortes vom Umfang des Alphabets (gleich Gesamtzahl der Flächen innerhalb der Maske) abhängig.

Die unregelmäßige Aufteilung der Graphik ist in der **Fig. 2** schematisch dargestellt.

Bei der technischen Realisierung des Verfahrens ist es wichtig zu beachten, daß nicht alle Verfahrensschritte hardwaremäßig innerhalb eines Gerätes oder am selben Ort durchgeführt werden müssen. So ist es insbesondere möglich, das Abspeichern des Zeichens, das Vergleichen des Zeichens der ausgewählten Region mit dem abgespeicherten Zeichen und das Feststellen der Identität des Benutzers, falls das Zeichen der ausgewählten Region mit dem abgespeicherten Zeichen übereinstimmt, auszulagern. Insbesondere kann dies auf herkömmlichen Geräten erfolgen.

Patentansprüche

1. Verfahren zur Identitätsprüfung, umfassend die folgenden Schritte:
   - erstes Anzeigen eines sichtbar oder unsichtbar in verschiedene Regionen gegliederten Bildes;
   - Zuordnen eines alphanumerischen od. dgl. Zeichens zu der von einem Benutzer bei einer Ersteingabe ausgewählten, mindestens einen Region;
   - Abspeichern des Zeichens;
   - Anzeigen des unsichtbar in verschiedene Regionen gegliederten Bildes;
   - Zuordnen eines alphanumerischen od. dgl. Zeichens der von dem Benutzer bei einer folgenden Eingabe ausgewählten, mindestens einen Region;
   - Vergleichen des Zeichens der ausgewählten Region mit dem abgespeicherten Zeichen und
   - Feststellen der Identität des Benutzers, falls das Zeichen der ausgewählten Region mit dem abgespeicherten Zeichen übereinstimmt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß mehrere Regionen bei der Ersteingabe ausgewählt, die entsprechenden Zeichen gespeichert und bei einer folgenden Eingabe mit den Zeichen der dann ausgewählten Regionen verglichen werden.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß bei der Ersteingabe auch die Reihenfolge der Zeichen der ausgewählten Regionen abgespeichert wird und der Zugang nur dann gewährt wird, wenn auch die Reihenfolge der Zeichen der von dem Benutzer bei einer folgenden Eingabe ausgewählten Regionen mit der abgespeicherten Reihenfolge der Zeichen übereinstimmt.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Zeichen der Regionen bei der Ersteingabe und den weiteren Verfahrensschritten nach Wahl des Benutzers aus verschiedenen Alphabeten entstammen.
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Alphabete ein Großbuchstaben- und ein Kleinbuchstabenalphabet umfassen.

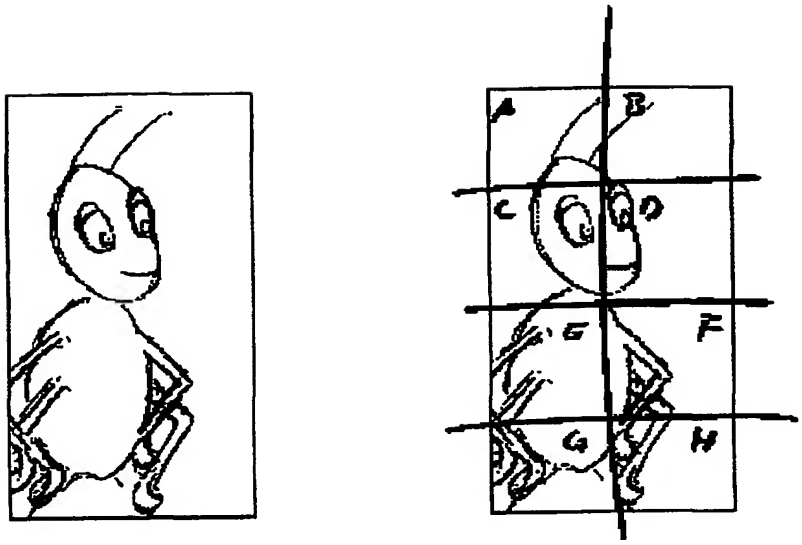
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß mehrere Bilder zur Auswahl stehen.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß ein Bild nach Auswahl durch einen ersten Benutzer für weitere Benutzer nicht mehr zur Auswahl steht.

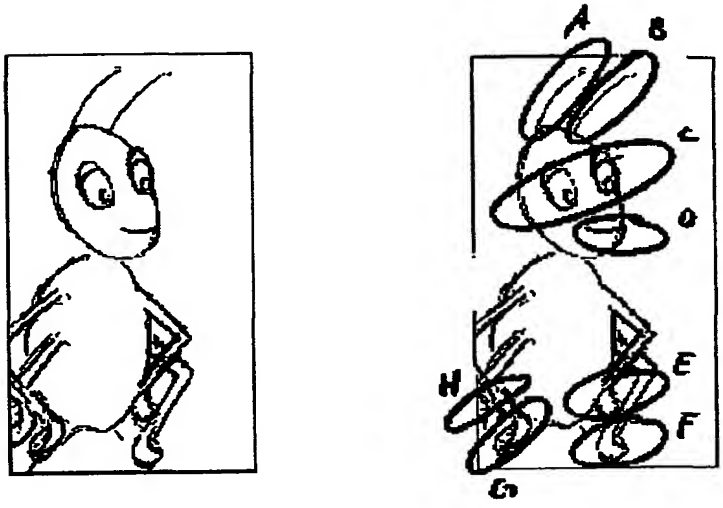
Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 198 48 501 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 4. Mai 2000



Figur 1 Regelmäßige Aufteilung der Graphik



Figur 2 Unregelmäßige Aufteilung der Graphik